KNOWiNK Poll Pad 2.5.0
Electronic Poll Book System
Security and Telecommunications Test Report for California

KNI-19001-STTR-02

Vendor Name	KNOWiNK
Vendor System	Poll Pad 2.5.0

Prepared by:

4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

Accredited by the Election Assistance Commission (EAC) for Selected Voting System Test Methods or Services

Revision History

Date	Release	Author	Revision Summary
January 30th, 2020	1.0	J. Peterson, J. Panek	Initial Release
February 14th, 2020	1.1	J. Peterson, J. Panek	Updates to address CA SoS comments

Disclaimer

The information reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government.

Trademarks

- SLI is a registered trademark of SLI Compliance.
- All products and company names are used for identification purposes only and may be trademarks of their respective owners.

TABLE OF CONTENTS

Test Report Overview

This Test Report details the full security and telecommunications review of the **KNOWiNK Poll Pad 2.5.0** electronic poll book system. An assessment of potential vulnerabilities is provided where applicable.

References

The following key documents were used in preparing this Test Report.

- California Electronic Poll Book Regulations.

Security and Telecommunications Review Process

The Security and Telecommunications review of the **KNOWiNK Poll Pad 2.5.0** electronic poll book system was conducted to analyze for findings against the following requirements:

- Examination of the top-level system design and architecture.
- Examination of the system documentation and procedures.
- Examination and open-ended testing of hardware, including when applicable, examination of unused hardware ports and the security measures to lock/seal hardware ports used. Physical testing may not be destructive. If a risk is identified that requires destructive testing, the contractor will discuss this and receive written approval from the Secretary of State before proceeding with a destructive test.
- Examination and open-ended testing of relevant software and operating system configuration.
- Examination and open-ended testing of system communications, including encryption of data, and protocols and procedures for access authorization.

The Security and Telecommunications testing was, to the maximum extent possible, conducted in a manner in which the testing began prior to having any knowledge of the source code to determine which vulnerabilities, if any, can be exploited without inside knowledge of the system.

Review Results and Analysis

SLI conducted a Security and Telecommunications review of the **KNOWiNK Poll Pad 2.5.0** electronic poll book system for compliance against the California Electronic Poll Book Regulations.

System Design and Architecture

The **KNOWiNK Poll Pad 2.5.0** electronic poll book system was examined for the top-level system design and architecture.

The expected outcome for this review was that no issue or discrepancies with respect to the requirements would be found.

The review determined that **KNOWiNK Poll Pad 2.5.0** utilizes Amazon Web Services to host the EPulse application and databases. Cisco Meraki hosts the application's Mobile Device Management (MDM) environment and Apple's enterprise development program digitally signs and distributes the application.

Each Poll Pad device is set up, deployed, and managed using the Cisco Meraki MDM.

The ePulse Administration web application is supported through utilization of AWS GovCloud, which provides in-depth infrastructure designed and managed to align with specific regulations, standards, and best practices for FIPS 140-2 and PCI DSS Level 1 requirements. All the security best practices are covered, including but not limited to:

- Physical and environmental security (Datacenter).
- Business continuity management.
- Secure network architecture.
- Database encryption (data at rest).
- Encrypted traffic: TLS 1.2, certificate authority signed certificates.
- AWS Shield: provides detection and mitigation of DDOS attacks.
- Firewalls locked down to allow only HTTP and HTTPS ports.
- Virtual Private Cloud to isolate backend server and database resources from the public.
- Application load balancing.
- Auto scaling for server resources during times of increased performance needs.
- Customizable security groups.
- Encrypted database management.
- CIS security benchmarks for server hardening.

Through the utilization of a mobile device management service provided by Cisco Meraki, the system allows all Poll Pads to be locked down to a specific level of access determined by the jurisdiction. This includes restrictions and functionality to:

- Limit access to install or uninstall applications.
- Control networking settings.
- Provide the ability to track, locate and remotely wipe Poll Pad devices.
- Provide the ability to monitor all Poll Pad device information, including connection state, model, IOS level, disk usage.

System Documentation and Procedures

The **KNOWiNK Poll Pad 2.5.0** electronic poll book system was examined for system documentation and procedures.

The expected outcome for this review was that no issue or discrepancies with respect to the requirements would be found.

The actual outcome for this review was a determination that the supplied documentation adequately details setup and configuration of the system. The documentation includes both setup of the physical configuration, including pairing the Bluetooth printers, and setup of the Poll Pad for use during an election.

Documentation also describes the setup and use of the application, including updating the application using Cisco Meraki's MDM and documentation for ePulse management and use.

The review determined that supplemental documentation provides an adequate overview of security features provided by the 3rd party service providers Apple IPAD security, Cisco Meraki, and Amazon Web Services.

Documentation on processes, procedures, and telecommunications ability was reviewed for the overall design and architecture of the system.

Hardware

The **KNOWiNK Poll Pad 2.5.0** electronic poll book system was examined for hardware, including, where applicable, examination of unused hardware ports and the security measures to lock/seal hardware ports used. Physical testing was not destructive.

The expected outcome for this review was that no issue or discrepancies with respect to the requirements would be found.

The **KNOWiNK Poll Pad 2.5.0** electronic poll book system incorporates a proprietary cover and stand that does not have built-in protective measures around the lightning port or the 3.5mm headphone jack. The protective case doesn't block or inhibit the on/off – sleep/wake button, the volume up/down buttons, or the built-in

camera and stereo speakers. The lack of physical port protection or button control doesn't hinder the overall security of the Poll Pad device due to additional management and security features that allow remote location discovery, the ability to lock the iPad device, and the ability to remotely wipe data.

Each Poll Pad device and accessories are packaged in a padded carrying case that supports the use of security seals and/or padlocks to ensure secure transportation and delivery of the solution. The provided solution presents a tamper-evident storage environment if warranted.

The padded carrying case and proprietary cover/stand were not provided for this testing engagement; however, they were evaluated in previous certification testing. The testing team confirmed with the manufacturer that those items are unchanged with this version of the system.

Inspection of the Bluetooth Wireless Star Micronics TSP650 printer determined that there were no additional security concerns from external port manipulation. There is an RJ-11 port that is used for receipt printer accessories such as a kitchen buzzer, ticket alarm, or drawer kick. All attempts to compromise the printer from this port were unsuccessful.

Inspection of the Bluetooth Wireless Brother Pocket JET PJ-763MFi printer determined that there was an unprotected USB Mini-b connector. This connector could be used to physically connect the printer to other devices which, in and of itself, is not considered a vulnerability.

It should be noted that jurisdictional polling place security processes and procedures play a large role in making sure that the **KNOWiNK Poll Pad 2.5.0** electronic poll book system remains secure. This would include processes and procedures for implementation of each device for use by poll workers in each jurisdiction, as well as physically securing each device before, during and after the election process.

Software and Operating System

The **KNOWiNK Poll Pad 2.5.0** electronic poll book system was examined and tested for relevant software and operating system configuration.

The expected outcome for this review was that no issue or discrepancies with respect to the requirements would be found.

The outcome for this review has confirmed that the system delivered and set up is the ePulse Management system, and the Poll Pads are configured per the KNOWiNK documentation for running voter check-in services.

- The backend setup and configuration for the ePulse Amazon Web Services instance backend were not verified as this configuration is hosted on AWS equipment.

- Detailed documentation was not provided for the setup and management of the backend server instance infrastructures.
- ICS Benchmarks were used to set up and harden AWS.
- Cisco Meraki MDM was utilized to manage and configure iPad devices.

The following systems and services were reviewed for relevant software and system configuration:

- Cisco Meraki MDM was utilized to manage and configure iPad devices.
- The EPulse Central Command utilizes AWS GOVCloud. The system utilizes AWS VPC (Virtual Public Cloud) to isolate all network traffic within the backend server instance environment from public access. EPulse connectivity is only allowed on HTTP and HTTPS ports; all HTTP traffic is automatically redirected to HTTPS.
- iPad IOS communication security best practices for setup.
- Bluetooth connectivity.

System Communications

The **KNOWiNK Poll Pad 2.5.0** electronic poll book system was examined and tested for system communications, including encryption of data, and protocols and procedures for access authorization.

The expected outcome for this review was that no issue or discrepancies with respect to the requirements would be found.

The physical communications equipment used by the system is split up into distinct communications systems.

- iPad Device (Poll Pad) zero-configuration peer-to-peer communications Bonjour service.
- Bluetooth connectivity including iPad and receipt printer (STAR TSP650 II, Brother PocketJet PJ-763MFi).
- Wireless network (MiFi, Cellular, WPA2 networking).
- AWS network connectivity.

Utilizing resources from KNOWiNK and industry documentation for COTS and third-party services, the following items were reviewed.

- Peer-to-Peer network communications:
  - iPad specific communications leverage out-of-the-box security measures, controlled by a Mobile Device Management system.
  - Utilization of the IOS Bonjour discoverable sockets. The Poll Pad application allows the ability for each iPad to utilize peer-to-peer networking in a secure encrypted fashion. EPulse controls encryption and initial setup match records for each Poll Pad device.

- Cisco Meraki MDM:
  - Ability to control network connectivity settings based upon jurisdiction network requirements.
  - Ability to restrict network communications.
- Bluetooth communications:
  - Apple IOS Bluetooth security.
  - Epson Model M335B receipt printer Bluetooth.
- Wireless communications:
  - Wireless connectivity (WPA2).
  - MiFi Communications devices.
  - Cellular communications.
- AWS Services:
  - Encrypted traffic: TLS 1.2 certificate authority signed certificates.
  - AWS Shield: provides detection and mitigation of DDOS attacks.
  - Firewalls locked down to allow only HTTP and HTTPS ports.
  - Virtual Private Cloud to isolate backend Server and Database resources from the public.

It was determined that for each of the communications systems, the system design and architecture are within the California Electronic Poll Book security requirements.

Findings

This section discusses findings from the **KNOWiNK Poll Pad 2.5.0** electronic poll book system Security and Telecommunications Review, as well as potential impacts.

Security and Telecommunications Review Discrepancies

At the time of the review there were no discrepancies found. All portions of the communications systems were configured per the documentation.

Vulnerabilities

To the extent possible, reported vulnerabilities include identification of the applicable requirement as well as an indication of whether the exploitation of the vulnerability would require access by:

- Voter: Usually has low knowledge of the Electronic Poll Book System's software and/or hardware design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others.

- Poll worker: Usually has low knowledge of the Electronic Poll Book System's software and/or hardware design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the software and/or hardware for up to ten days, but all physical security has been put into place before the machines are received.
- Elections official insider: Wide range of knowledge of the Electronic Poll Book System's software and/or hardware design and configuration. May have unrestricted access for long periods of time. Their designated activities include:
  - Setup and pre-election procedures;
  - Election operation;
  - Post-election procedures; and
  - Archiving and storage operations.
- Vendor insider: With great knowledge of the Electronic Poll Book System's software and/or hardware design and configuration. They have unlimited access to the Electronic Poll Book System's software and/or hardware before it is delivered to the purchaser and, thereafter, may have unrestricted access when performing warranty and maintenance service and when providing election administration services.

SLI will not verify or demonstrate exploitability of the vulnerability, but the report of the vulnerability will identify factors involved in the exploitation. Any vulnerability theories developed by the security team members are, to the extent possible, provided to the Secretary of State staff herein.

Vulnerabilities Found

The findings for vulnerabilities are organized into two sections: the ePulse control center and the Poll Pad technology.

ePulse

1. Cross-site scripting (DOM-Based) (Severity: High – Confidence: Tentative: Determined by static code analysis, which may lead to false positives)

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based cross-site scripting arises when a script writes controllable data into the HTML document in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to visit the attacker's crafted URL in various ways, similar to the usual attack delivery vectors for reflected cross-site scripting vulnerabilities.

2. **Open redirection (DOM-Based) (Severity: Low – Confidence: Tentative: Determined by static code analysis, which may lead to false positives)**

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

3. **Cookie scoped to parent domain (Severity: Low – Confidence: Firm)**

A cookie's domain attribute determines which domains can access the cookie. Browsers will automatically submit the cookie in requests to in-scope domains, and those domains will also be able to access the cookie via JavaScript. If a cookie is scoped to a parent domain, then that cookie will be accessible by the parent domain and also by any other subdomains of the parent domain. If the cookie contains sensitive data (such as a session token) then this data may be accessible by less trusted or less secure applications residing at those domains, leading to a security compromise.

4. **Password field with autocomplete enabled (Severity: Low – Confidence: Certain)**

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability

such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

5. **Link manipulation (DOM-based) (Severity: Low – Confidence: Firm; Determined by static code analysis, which may lead to false positives)**

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

DOM-based link manipulation arises when a script writes controllable data to a navigation target within the current page, such as a clickable link or the submission URL of a form. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the target of links within the response.

6. **Content Type incorrectly stated (Severity: Low – Confidence: Firm)**

If a response specifies an incorrect content type, then browsers may process the response in unexpected ways. If the content type is specified to be a renderable text-based format, then the browser will usually attempt to interpret the response as being in that format, regardless of the actual contents of the response. Additionally, some other specified content types might sometimes be interpreted as HTML due to quirks in particular browsers. This behavior might lead to otherwise "safe" content such as images being rendered as HTML, enabling cross-site scripting attacks in certain conditions.

The presence of an incorrect content type statement typically only constitutes a security flaw when the affected resource is dynamically generated, uploaded by a user, or otherwise contains user input.

7. **Strict transport security not enforced (Severity: Low – Confidence: Certain)**

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer.

Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack.

Poll Pad

While no specific vulnerabilities were found in the examination of the iPad technology used to run the Poll Pad application, the application and iPad hardware utilize Bluetooth technology to connect to Bluetooth receipt printers. All attempts to compromise the iPad and the receipt/ballot printer were unsuccessful beyond basic reconnaissance data being pulled from the Bluetooth devices. The limited connectivity range helps to minimize the impacts of attacks against these devices.

Each of the iPad devices utilize Apple’s zero configuration peer-to-peer networking service to keep Poll Pads located within the same physical location up to date on voter check-in. All attempts to sniff, access, or compromise this network were unsuccessful.

Conclusions

Seven vulnerabilities were located within the **KNOWiNK Poll Pad Plus 2.5.0** electronic poll book system, related to the ePulse Administration web application. These vulnerabilities ranged in severity from low to high. All vulnerabilities discovered were considered of minimal impact to the overall security of the **KNOWiNK Poll Pad Plus 2.5.0** electronic poll book system. The web vulnerability scan of the application was completed using an administrative credentialed account.

Nessus scans indicated that there were only informational vulnerabilities discovered about the ePulse web backend. There was one informational related vulnerability that should be noted regarding use of a weak hashing algorithm. Details of this informational vulnerability are described below.

It should be noted that the system relies upon security measures that are dependent upon third party technology and services, including Apple native IOS Security, Cisco Meraki MDM, and Amazon Web Services. Compromise to the individual systems and services could affect the overall security of the system.

It should be noted that the systems tested onsite utilize wireless communications of any type and that if the system is not set up to the specific requirements of the jurisdiction, improper configuration could lead to compromise of the system. Use of unsecure/unauthorized networks is an example.

It should also be noted that the system uses both Bluetooth and peer-to-peer wireless communications to keep Poll Pad devices connected to each other for real time sharing of check-in data between polling place devices. Reasonable attempts were made to sniff, access, or compromise these networks and the attempts were unsuccessful.

While not full-blown vulnerabilities, the following items could lead to issues or compromise if not properly monitored:

- Bluetooth Pair and Reset buttons on the Bluetooth receipt printer and ballot printer were accessible. Access to these buttons may result in Bluetooth pairing/connectivity issues.
- The STAR TSP650 Receipt Printer DK port, which is used to send a signal to open a cash drawer upon receipt generation, is currently not in use. Attempts to compromise this port were unsuccessful.
- The Brother PocketJet PJ-763MFi blue tooth ballot printer has an unprotected USB Mini-b port.
- Any Wi-Fi networking used by the jurisdictions is subject to processes and procedures set forth by the jurisdiction and was not specifically tested or reviewed.

Testing was conducted in an attempt to circumvent or exploit vulnerabilities within the communication systems such as applicable and within legal boundaries in respect to third party services.

The iPad devices sufficiently meet requirements by:

- Offering FIPS-140-2 encryption to data both at rest and during transmissions utilizing AES 256Bit encryption or greater.
- Giving precise control of all aspects of the iPad device configuration using Mobile Device Management.
  - Ability to remotely wipe iPad devices.
  - Ability to track lost or stolen devices.
  - Control of Wi-Fi access.
  - Control of application versions.
- Allowing for separate environments designed to protect each application from infecting or compromising another through the use of Application Sandbox.
- Providing the ability to lock down the iPad device to a single application using guided access (KIOSK) mode.

End of Test Report